Individual Certification of Security Proficiency for Software Professionals: Where Are We? Where Are We Going?

Dan Shoemaker, Centre for Assurance Studies [vita[1]]

2009-01-23

The software industry needs a universally acknowledged credential to document that a software professional has all of the requisite knowledge and skills to produce a secure product. This article describes some of the existing professional certifications in information assurance and emerging certifications for secure software assurance.

Introduction: Reassuring Trust

The person who cuts my hair has a certificate that says she is proficient to do that. The same is true for the person who fixes my car and plumbs my pipes. Those formal proofs of competency are very reassuring, since delicate items like my car, my house, and what is left of my hair are very important to me. On the other hand, it is an almost certain bet that the people who wrote the computer program that I am using cannot document that they are capable of writing secure code. And it certainly doesn't do good things for my level of trust to find out that the software industry doesn't require any type of formal proof that its workers can produce a secure product.

When the only problem facing the industry was product quality, it might have been acceptable to let software people build products without first finding out whether they were competent to do the work. However, we can't afford to be so accommodating now that the exploitation of a single flaw could conceivably bring down our entire cyber infrastructure. That leads us to the thesis of this article. Given the critical importance of software in our society, the profession has to find a standard, commonly accepted way to certify the security knowledge of its workforce.

Notwithstanding the fact that the ability to ensure our products at some minimally acceptable level of trust is important to national security, common, industry-wide certification of individual capability would be a valuable business tool. It would let organizations know what abilities they were actually hiring. Even better, it would also let managers manage software work with certainty, since they would know in advance who was capable of producing secure products and more importantly who was *not*.

A Common Proof of Security Competency for Software Professionals

The key concepts in this discussion are the terms "security" and "commonly accepted." Certification in the computer industry is a very profitable business. In fact, since the 1980s certificates spanning the alphabet from "A+" to "Ubuntu Certified Professional" have become something of a cottage industry in the profession

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/689-BSI.html (Shoemaker, Dan)
[2] #dsy1090-BSI_intro
[3] #dsy1090-BSI_common
[4] #dsy1090-BSI_popular
[5] #dsy1090-BSI_emerg
[6] #dsy1090-BSI_conclu

[Webopedia 2008[7]]. That profit motive probably also explains why over 200 new certificate products were added to an already overpopulated field in the past ten years [IEEE 2008[8]].

Nonetheless, what we are discussing here is the need for a universally acknowledged credential to document that a software professional has all of the requisite knowledge and skills to produce a secure product. Right now, there are vendor or product specific certifications out there that relate to some aspect of securing a computer, such as networks, operating systems, and even applications [MC MCSE 2008[9]]. The problem is that none of the products on the market right now certifies an individual's knowledge of secure development, sustainment, or acquisition practice [MC MCSE 2008[10]].

The idea of an omnibus certificate of security capability is a relatively new concept in the field of software. However, it is not a new idea in the overall field of information assurance. That is due the fact that, over the past 30 years, the professional capabilities of professionals in that field have been underwritten by a number of established credentials. These certifications document that the holder possesses "a common understanding of the concepts, principles, and applications of IA."

Information Assurance Professional Certification Examples

The actual certification of competency in information assurance is underwritten by a long list of well-validated and standard certification tests. Vendors on that list include ISC2, ISACA, SANS, CompTIA, and many others. As examples, some of these certifications are described below.

The Certified Information Systems Security Professional (CISSP)

The CISSP is granted by examination and based on experience requirements [ISC2 2008[11]]. The exam is derived from the CISSP Common Body of Knowledge (CBK), which encapsulates ten domains, or areas of information assurance knowledge. These ten domains are considered comprehensive for IA work. The ten CISSP-CBK domains are [ISC2 2008[12]]

1. Access Control
2. Application Security
3. Business Continuity and Disaster Recovery Planning
4. Cryptography and Cryptanalysis
5. Policies and Procedures for Information Security and Risk Management
6. Legal, Regulations, Compliance and Investigations
7. Operations Security
8. Physical (Environmental) Security
9. Principles and Practices of Security Architecture and Design
10. Telecommunications and Network Security

One of the features of the CISSP is the requirement that it be renewed every three years. That renewal is generally based on the holder's ability to document 120 Continuing Professional Education (CPE) credits since the previous renewal. These credits are typically derived from formal continuing education conferences.

[7] #dsy1090-BSI_webo08
[8] #dsy1090-BSI_ieee08
[9] #dsy1090-BSI_mcse08
[10] #dsy1090-BSI_mcse08
[11] https://buildsecurityin.us-cert.gov/daisy/adm-bsi/articles/best-practices/training/1090-BSI/edit/3d068a535f28436f7248052b5140838055507d72/part-article-body#isc208
[12] #dsy1090-BSI_isc208

The Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM)

These are both certification products of the Information Systems Audit and Control Association (ISACA). Both of these certifications are based on knowledge captured in a four domain, control objective based model called COBIT. The four domains of COBIT are [ISACA 2008b[13]]

1. Domain One: Planning and Organization
2. Domain Two: Acquisition and Implementation
3. Domain Three: Delivery and Support
4. Domain Four: Monitor

Each of the 34 high-level control processes that comprise these domains is implemented by anywhere from 3 to 30 specific control objective activities, amounting to 318 total standard activities specified for control of IT and information assets [ISACA 2008b[14]].

The CISA is the more common of these two certificates, since it predates the CISM by 25 years. Since the focus of both of these certificates is on explicit and documentable controls rather than best practices for security, the CISA in particular has more of an accounting and business flavor than the technical and practitioner feel of the CISSP. Like the CISSP, however, the CISA documents a specific set of skills and practices oriented toward ensuring the confidentiality, integrity, and availability of information. On the other hand, the CISM certification is oriented toward the assurance of information itself.

The CISA was introduced in 1978, while the CISM was introduced in 2003 [ISACA 2008a[15]]. As the name implies, the CISM is designed for managers, designers, and overseers of an organization’s overall information security program. Thus, the knowledge and competencies certified by the CISM are more oriented toward the fulfillment of the management responsibilities for information assurance rather than the technical aspects of the profession.

The SANS Global Information Assurance Certification (GIAC)

Like the CISSP, GIAC is a practitioner certificate designed to validate real-world skills. Its intent is to “provide assurance that a certified individual has practical awareness, knowledge and skills in key areas of computer and network and software security” [SANS 2008[16]].

The GIAC is much more of a technical credential than the CISSP and the CISA/CISM. Also, the GIAC specifically documents capabilities for over 20 types of professional areas [SANS 2008[17]]. So in that respect the GIAC is more of a series of potential certifications that an individual can earn rather than a general-purpose certificate of information security knowledge. This fact should be kept in mind in the discussion in the next section.

Certifications for the Field of Secure Software Assurance

More recently we have observed an increase in training courses and certifications for secure software development. It is not surprising that some of the same organizations with certification products in information assurance would migrate into the field of software assurance. At present, two certifications are being developed for two different client bases in the secure software assurance community. Examples of organizations that are offering software assurance certifications are ISC2 and SANS.

[13] #dsy1090-BSI_isaca08b
[14] #dsy1090-BSI_isaca08b
[15] #dsy1090-BSI_isaca08a
[16] #dsy1090-BSI_sans08
[17] #dsy1090-BSI_sans08

Certified Secure Software Lifecycle Professional (CSSLP)

The CSSLP parallels the CISSP in that it takes a holistic view of the entire process of software development. As such, it is a general assessment of an individual’s general security competency across the entire software life cycle. Like the CISSP, the CSSLP assesses breadth of knowledge rather than depth in any particular area. The CSSLP is based on a set of general best practices for secure software assurance, which are organized into seven domains [ISC2 2008[18]]. These domains are

1. Secure Software Concepts - security implications across the life cycle
2. Secure Software Requirements – how to elicit security requirements
3. Secure Software Design – how to embed security requirements in design
4. Secure Software Implementation/Coding - security functionality testing, secure code development, attack and exploit mitigation
5. Secure Software Testing - testing for robustness and security functionality
6. Software Acceptance – getting security into the software acceptance phase
7. Software Deployment, Operations, Maintenance and Disposal – how to securely sustain software throughout its useful life cycle

Like the CISSP, practitioners will have to prove that they have three or four years of professional experience in secure software work. The proof of competence will come from a qualifying exam that is administered similar to that of the CISSP. The first of these is planned for June of 2009 [Schneider 2008[19]]. In addition, once the CSSLP has been granted to an individual, the certification must be maintained through continuing education [ISC2 2008[20]].

Like the CISSP, the CSSLP is an attestation to a broad range of minimum competency in secure software work, rather than in-depth substantiation of mastery in some particular aspect of that work.

The SANS Secure Coding Assessment

The SANS Secure Coding Assessment, which is a part of the overall SANS Software Security Institute, is designed to certify that the holder has the requisite set of skills in secure coding. In this case, the objective is for the holder to achieve GIAC Secure Software Programmer (GSSP) Certification. This is done through an exam process similar to the ones utilized by SANS in the information assurance areas.

That is, rather than being a general assessment, these exams are tailored to specific applications. In the case of the basic CSSP, it is possible for holders to be certified in four specific programming languages. These are C/C++, Java/J2EE, Perl/PHP, and .NET/ASP [SANS 2008[21]]. Like the other certifications, holders of the GSSP have to recertify, in this case every four years. Current holders have to pass the test that is being utilized at the time of their recertification [SANS 2008[22]].

According to SANS, these tailored certifications will help organizations meet four distinct objectives [SANS 2008[23]]. First, the exam can serve as a yardstick by which an organization can measure the individual security knowledge of its programmers. That knowledge can then be leveraged into focused training for each person. Second, the exam will also allow the organization to ensure that any outsourced work is done by programmers who have a requisite level of security knowledge. Third, it will help an organization structure its hiring processes to ensure that people who are brought into the organization are competent to start work on day one, without additional costly training. Finally, it will allow organizations to make more effective and efficient project assignments by identifying individuals with advanced security skills.

[18] #dsy1090-BSI_isc208
[19] #dsy1090-BSI_schn08
[20] #dsy1090-BSI_isc208
[21] #dsy1090-BSI_sans08
[22] #dsy1090-BSI_sans08
[23] #dsy1090-BSI_sans08

Given SANS's traditional focus on technology, the desired effect of this certification will be to provide attestation to the holder's ability to find and fix common errors that lead to security vulnerabilities in each of the languages in which they are certified. That will allow managers to ensure a base level of security knowledge in each project, and it will also help employers more objectively evaluate potential candidates for employment. Finally, it should also serve as a comparative basis for those organizations with a large proportion of GSSPs on their staff, to prove their worth when competing for business.

Concluding Remarks

The problem of understanding what the huge variety of certificates means represents one of the chief hazards in using information assurance certification as a proof of capability. Because there are so many certificates and because they mean different things, it is difficult for the general population to tell what they are getting when they hire a CISA versus a CISSP, or a Security Plus versus a GIAC. In order to address that exact question, the Office of Cybersecurity and Communications, which is located within the DHS National Cyber Security Division (NCSD), has released a document entitled the Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development [DHS 2008[24]]. This document represents a solid first attempt to create a single point of reference to understand the range of personal certifications. However, the EBK addresses the entire field of information security, not expressly secure software assurance.

In the same vein, the Department of Defense has issued a revision to DoD 8570.01-M [DoD 2008[25]]. DoD 8570 specifies the knowledge and certification requirements for the employees of the Department of Defense. This directive is important because it requires every full- and part-time military service member, defense contractor, civilian, and foreign employee with privileged access to a DoD system to obtain a commercial certification credential. In that respect, it is the first example of an across the board standardization of competency for security. Because the commercial credential must be certified to ISO/IEC 17024 [ISO/IEC 2003[26]] in order to be valid, DoD 8570 ensures that employees of the Department of Defense all fit within a commonly accepted framework for workforce capability. However, like the EBK, 8570 only deals with competencies for the general field of information assurance.

Governmental and industry leaders might want to think about characterizing the global knowledge and skills necessary to ensure secure software competency, much in the same way that the EBK does for information security. Given the history of certification, it would be far preferable to have that discussion now rather than several years down the road when the secure software certification landscape has become a wilderness.

Bibliography

[DHS 2008]

Department of Homeland Security. "IT Security Essential Body of Knowledge[27] (EBK): A Competency and Functional Framework for IT Security Workforce Development," Sept. 2008.

[DoD 2008]
Department of Defense. "DoD 8570.01-M, Information Assurance Workforce Improvement Program," December 19, 2005; Revised, May 15, 2008.

[IEEE 2008]
IEEE. "CSDP, Is Certification Right for You? Certification Road Map: The Journey and the Destination." IEEE Computer Society[28], 2008.

[ISACA 2008a]

[24] #dsy1090-BSI_dhs08
[25] #dsy1090-BSI_dod08
[26] #dsy1090-BSI_iso03
[27] http://www.us-cert.gov/ITSecurityEBK/
[28] http://www.computer.org/portal/site/ieeecs/index.jsp

Information Systems Audit and Control Association (ISACA). “Certification Overview.” ISACA[29], Oct. 2008.

[ISACA 2008b]
Information Systems Audit and Control Association (ISACA). “Control Objectives for IT (COBIT).” ISACA[30], Oct. 2008.

[ISC2 2008]
International Information System Security Certification Consortium (ISC2). “CSSLP –Certified Secure Software Lifecycle Professional[31]," Nov. 2008.

[ISO/IEC 2003]
International Standards Organization/International Electronics Commission. *ISO/IEC 17024 - General Requirements for Bodies Operating Certification of Persons*, April 2003.

[MC MCSE 2008]
MC MCSE. “Certification Resources[32],” 2008.

[SANS 2008]
SANS. “GIAC Secure Software Programmer[33],” 2008.

[Schneider 2008]
Schneider, Laura. “CSSLP – The Certified System Security Lifecycle Professional,” About.com[34], 2008.

[Webopedia 2008]
Webopedia. “Computer Certifications,” Sept. 17, 2008.

[Wikipedia 2008]
Wikipedia. “Certified Information Systems Security Professional[35] (CISSP),” 2008.

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[29] http://www.isaca.org/
[30] http://www.isaca.org/
[31] http://www.isc2.org/csslp/
[32] http://www.mcmcse.com/othercerts.shtml
[33] http://www.sans.org/gssp/
[34] http://www.about.com/
[35] http://en.wikipedia.org/wiki/CISSP
[1] mailto:permission@sei.cmu.edu